Organizadores:

Sponsors:

DATA & AI SUMMIT 2023

La ciencia de datos y la inteligencia artificial están cambiando cómo crear valor en las organizaciones. ¿Cómo sacar mayor provecho? Conversamos con dos especialistas que serán expositores en Data & AI Summit 2023.

“La ciberseguridad se está tomando como prioridad estratégica”

Chema Alonso, actual Chief Digital Officer de Telefónica. Es uno de los oradores sobre *hacking* y ciberseguridad más populares en todo el mundo.

¿Qué tendencias de ciberseguridad están ganando mayor presencia en las empresas de la región?

En la región, las empresas están adoptando soluciones de seguridad en la nube, gestión de identidades y accesos, educación de los empleados y tecnologías de inteligencia artificial y aprendizaje automático para protegerse contra las amenazas cibernéticas en evolución.

Pero lo más importante es el cambio en la prioridad en las empresas, ya que la ciberseguridad se está tomando como prioridad estratégica. Cada vez más organizaciones están reconociendo la importancia de la ciberseguridad como una necesidad fundamental para la continuidad del negocio y están invirtiendo en la implementación de medidas de seguridad adecuadas para proteger sus datos y sistemas con el objetivo final de proteger su negocio.

¿Cómo saber si las medidas de ciberseguridad adoptadas en mi empresa son las correctas?

Es importante realizar una evaluación exhaustiva de la seguridad de su sistema, identificar los riesgos y vulnerabilidades, verificar la implementación de las mejores prácticas de ciberseguridad y realizar pruebas y auditorías de seguridad para garantizar que las medidas de seguridad sean efectivas y estén actualizadas.

¿Cómo lograrlo?

Para ello, el equipo responsable de la seguridad (CISO) debe tener un sistema de gestión de riesgos que haya identificado correctamente los activos, lo riesgos, y las decisiones a tomar con cada uno de ellos. Después deberá implementar un plan director que permita implementar las mejores prácticas de seguridad, comprobarlas constantemente por medio de auditorías de seguridad constantes por parte de los equipos internos y externos gestionados por el Red Team, y luego evaluar diariamente los indicadores clave para saber si algo no está funcionando, está en riesgo o necesita una revisión.

Al final, la gestión de todos los equipos técnicos para prevenir ataques, detectarlos, responder y garantizar la resiliencia de la compañía contra todo lo que venga es la verdadera gestión de la ciberseguridad y por tanto, las medidas adoptadas deben estar sometidas a una revisión constante.

¿Cuáles son los errores más comunes que cometen las empresas en cuanto a ciberseguridad y cómo evitarlos?

El principal es no contar con un plan de seguridad definido que aborde los riesgos de ciberseguridad. Sin un plan sólido, las empresas no suelen implementar medidas de seguridad adecuadas, como la autenticación de dos factores, el cifrado de datos, la gestión de la identidad o la aplicación de parches de seguridad, que son necesarios para proteger sus sistemas contra vulnerabilidades conocidas.

¿Cómo repercute esto en la práctica?

Esto puede permitir que los ciberdelincuentes aprovechen las vulnerabilidades para atacar el sistema, y si sumamos una insuficiente formación y concienciación de los empleados sobre las mejores prácticas de seguridad, las tecnologías que utilizan o los últimos ataques, esto puede resultar en errores humanos que ponen en riesgo la seguridad de la compañía.

[Es decir] ¿cuántos empleados de tu empresa conocen cómo funciona OAuth, o cómo verificar un correo electrónico de phishing, o cómo funciona un ataque de un USB malicioso?

Por último, si la empresa no cuenta con un equipo de seguridad interno o externo, cuando pase algo, será un problema la identificación y respuesta a posibles amenazas.

Media partner :

Partner estratégico:

“Las consideraciones éticas deben estar presentes en todo desarrollo de inteligencia artificial”

Elena Estavillo, directora general de Centro-i para la sociedad del futuro. Es experta en el ecosistema digital y tecnológico, regulación, competencia y género.

¿Cuáles son los cuestionamientos éticos más críticos de cara a las empresas que genera la inteligencia artificial este 2023?
Algunas aplicaciones de inteligencia artificial incorporan sesgos pues estos sistemas aprenden de las decisiones y comportamientos humanos. Los mismos equipos que diseñan los algoritmos pueden incorporar sus propios sesgos a la inteligencia artificial si no están conscientes de estos riesgos o no tienen estrategias para contrarrestarlos.

Existen otros cuestionamientos que están relacionados con la privacidad y la seguridad de las personas, por la capacidad de la inteligencia artificial para analizar bases masivas de datos que relacionan sus características y sus comportamientos, lo que puede invadir su esfera privada e incluso generar riesgos para su seguridad.

¿Qué están haciendo las empresas para superar estos desafíos y qué más pueden hacer?
Algunas empresas comienzan a cuestionarse estos temas, pero queda mucho por hacer. La responsabilidad no está solo del lado de quienes producen la inteligencia artificial, sino también en las empresas que la usan.

Es importante que se informen sobre los posibles riesgos y evalúen desde ese punto de vista los sistemas que adquieren y aplican, además de que supervisen sus efectos. Inclusive, debe haber una reflexión ética sobre en qué casos los beneficios de la inteligencia artificial justifican sus riesgos.

¿Considera que la ciencia de datos y la inteligencia artificial pueden fortalecer los temas de ética dentro de las empresas? Si es así, ¿cómo lo hacen?
La ciencia de datos y la inteligencia artificial efectivamente pueden usarse con propósitos éticos. Esto ocurre cuando, desde su diseño, se buscan explícitamente propósitos de igualdad, transparencia, rendición de cuentas, justicia u otros; y haciendo una cuidadosa evaluación del impacto ético de los desarrollos tecnológicos.

¿Qué soluciones de la inteligencia artificial pueden ser aprovechados para mejorar resultados relacionados a inclusión, gobernanza y sostenibilidad dentro de las empresas?
Además de pensar en diseñar soluciones específicas para promover estos objetivos, las consideraciones éticas deben estar presentes en todo desarrollo de inteligencia artificial, desde el análisis de solicitudes de empleo, otorgamiento de crédito, evaluación de resultados, etc. Históricamente, en estos procesos ha habido sesgos y discriminación que pueden ser abordados por la inteligencia artificial con el objetivo explícito de corregirlos, a condición de que se trabaje desde las bases de datos, pasando por el diseño de algoritmos y la supervisión de los resultados.

El **Data & AI Summit 2023** se realizará los días **11, 12 y 13 de abril** en formato virtual. Para mayor información escribir a: **informes@seminarium.pe**